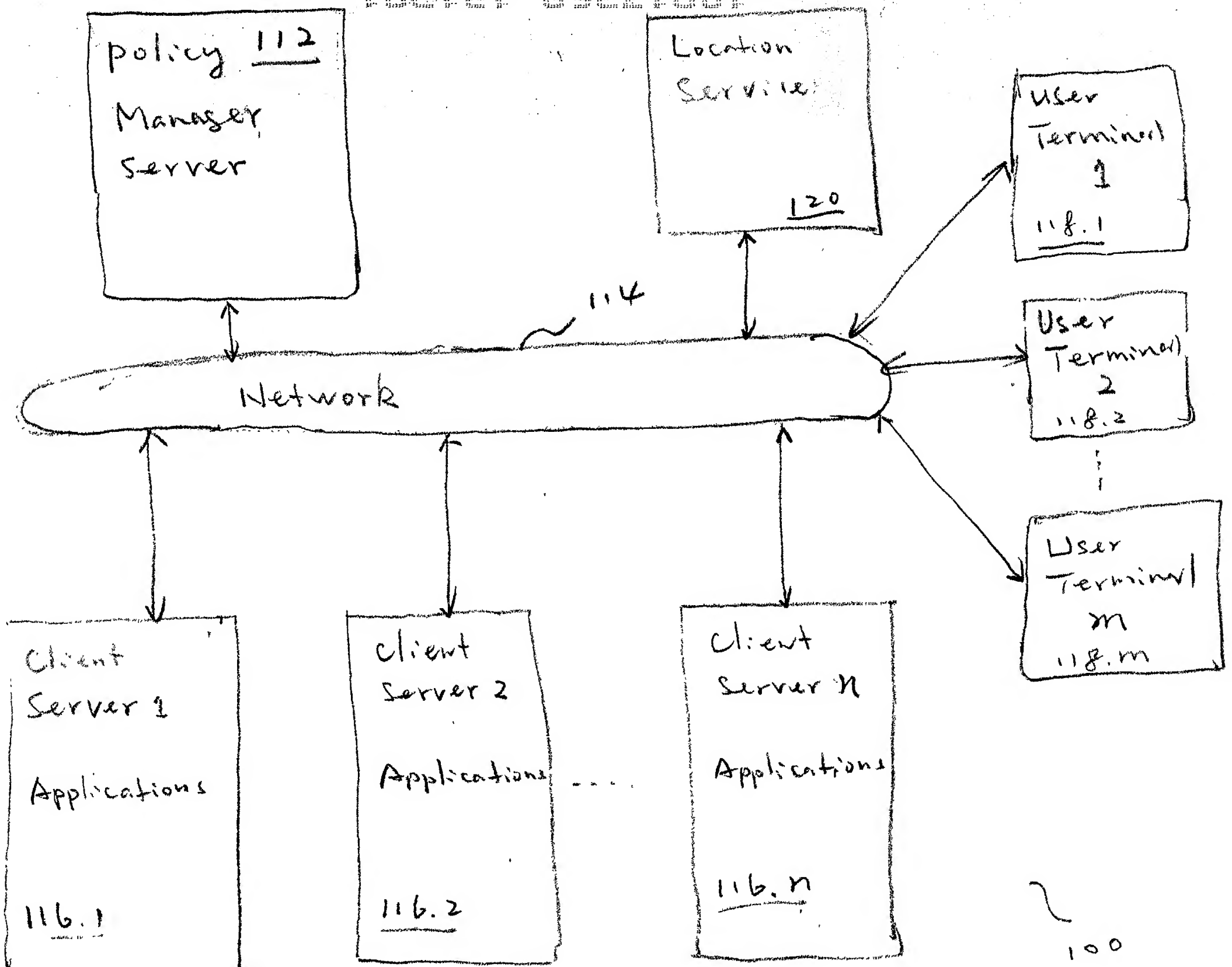

policy 112
Manager
Server
Location
Service
120
User
Terminal
1
118.1
114
Network
User
Terminal
2
118.2
User
Terminal
m
118.m
Client
Server 1
Applications
116.1
client
Server 2
Applications
116.2
Client
Server n
Applications
116.n
100

FIG. 1

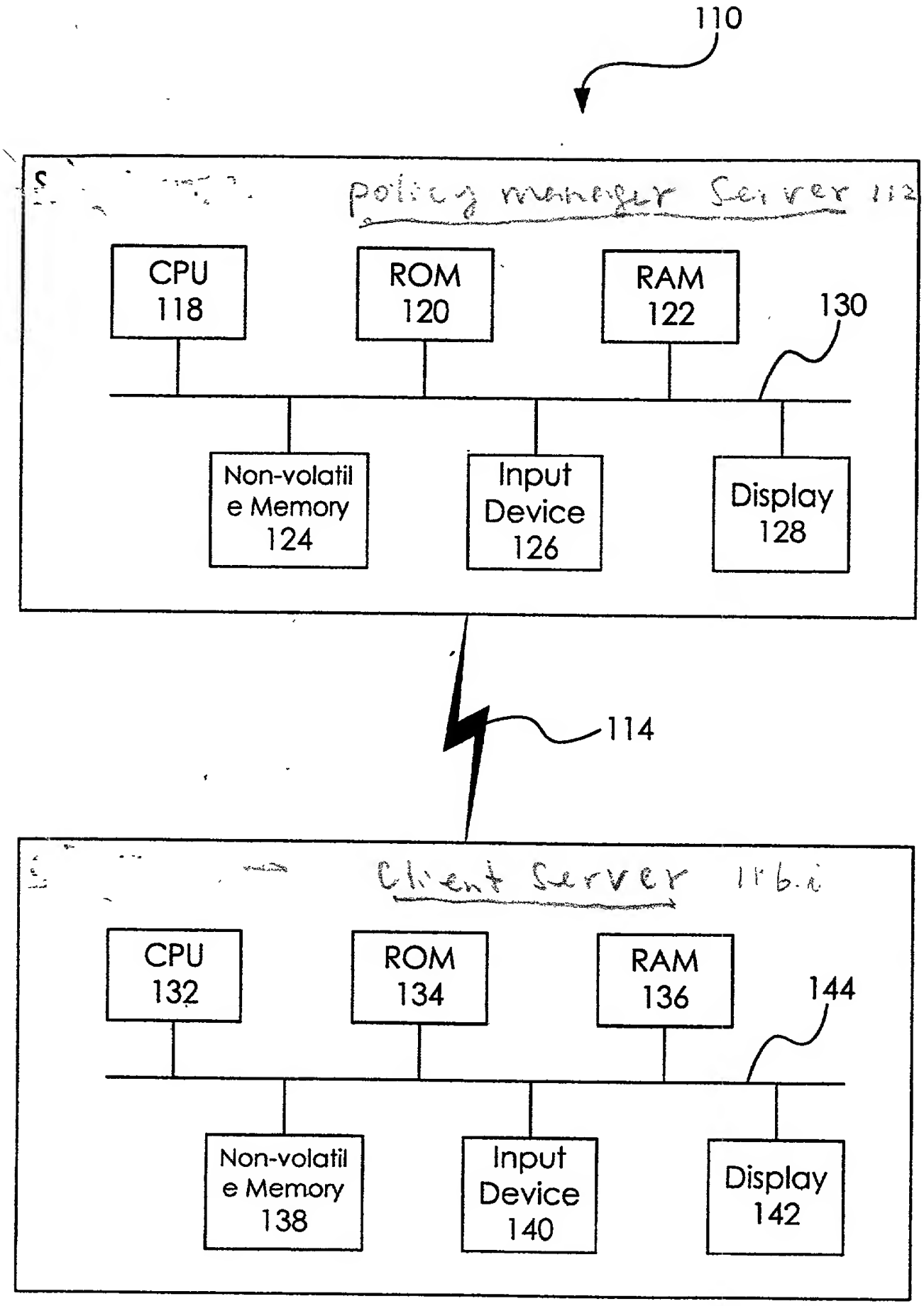

110
policy manager Server 112
CPU
118
ROM
120
RAM
122
130
Non-volatil
e Memory
124
Input
Device
126
Display
128
114
Client Server 116.i
CPU
132
ROM
134
RAM
136
144
Non-volatil
e Memory
138
Input
Device
140
Display
142

FIG. 1A

Policy Manager

SERVER

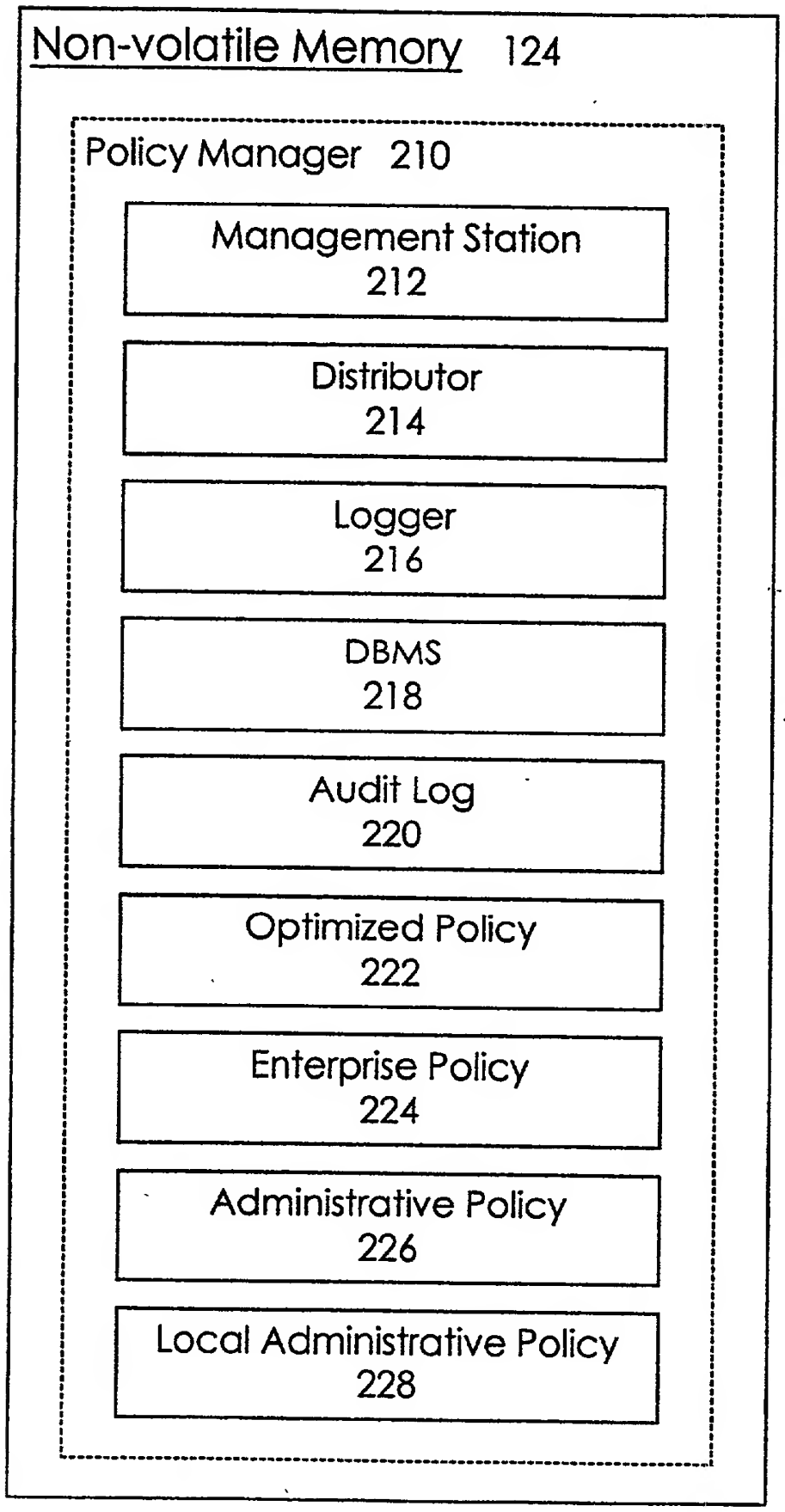


FIG. 2

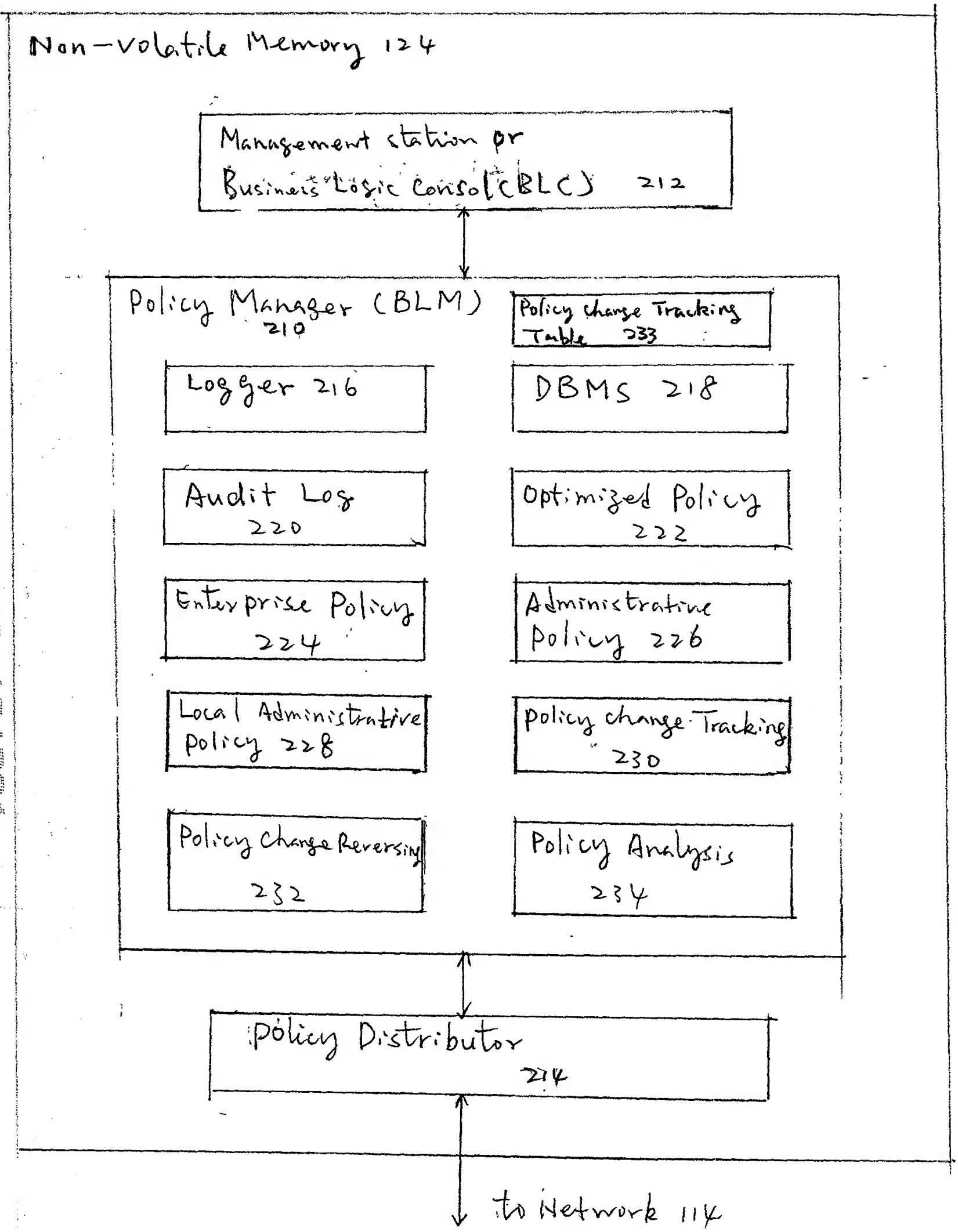

Non-volatile Memory 124
Management station or Business Logic Consol (BLC) 212
Policy Manager (BLM) 210
Policy change Tracking Table 233
Logger 216
DBMS 218
Audit Log 220
Optimized Policy 222
Enterprise Policy 224
Administrative Policy 226
Local Administrative Policy 228
policy change Tracking 230
Policy Change Reversing 232
Policy Analysis 234
Policy Distributor 214
to Network 11K

FIG. 2A

CLIENT Server

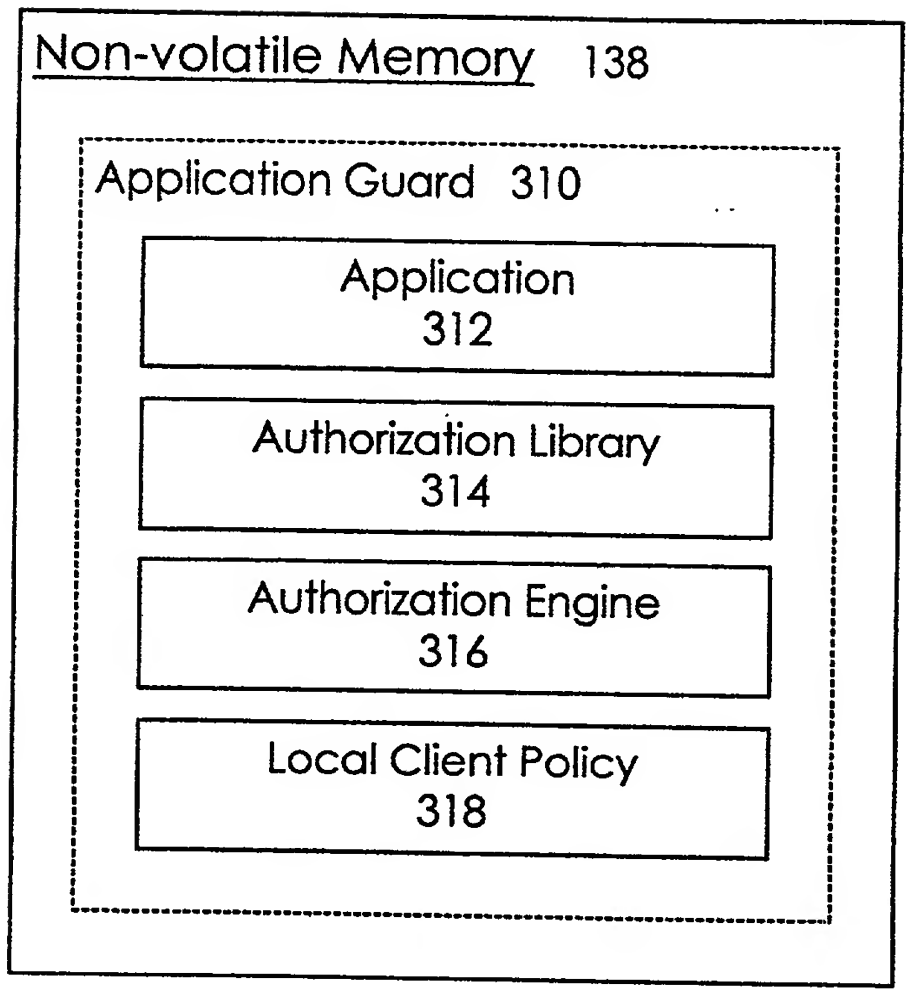


FIG. 3

Client Server

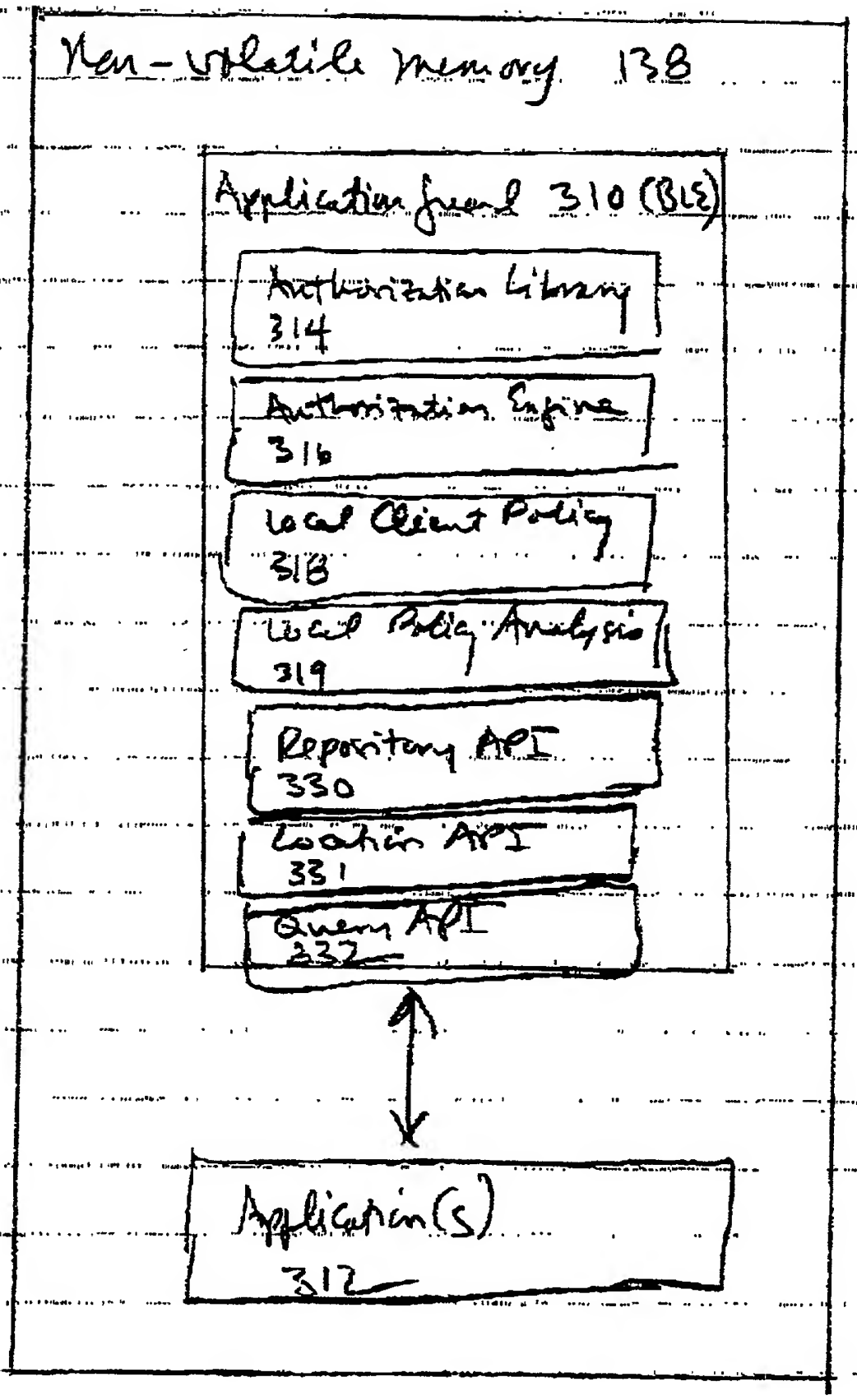


Fig. 3A

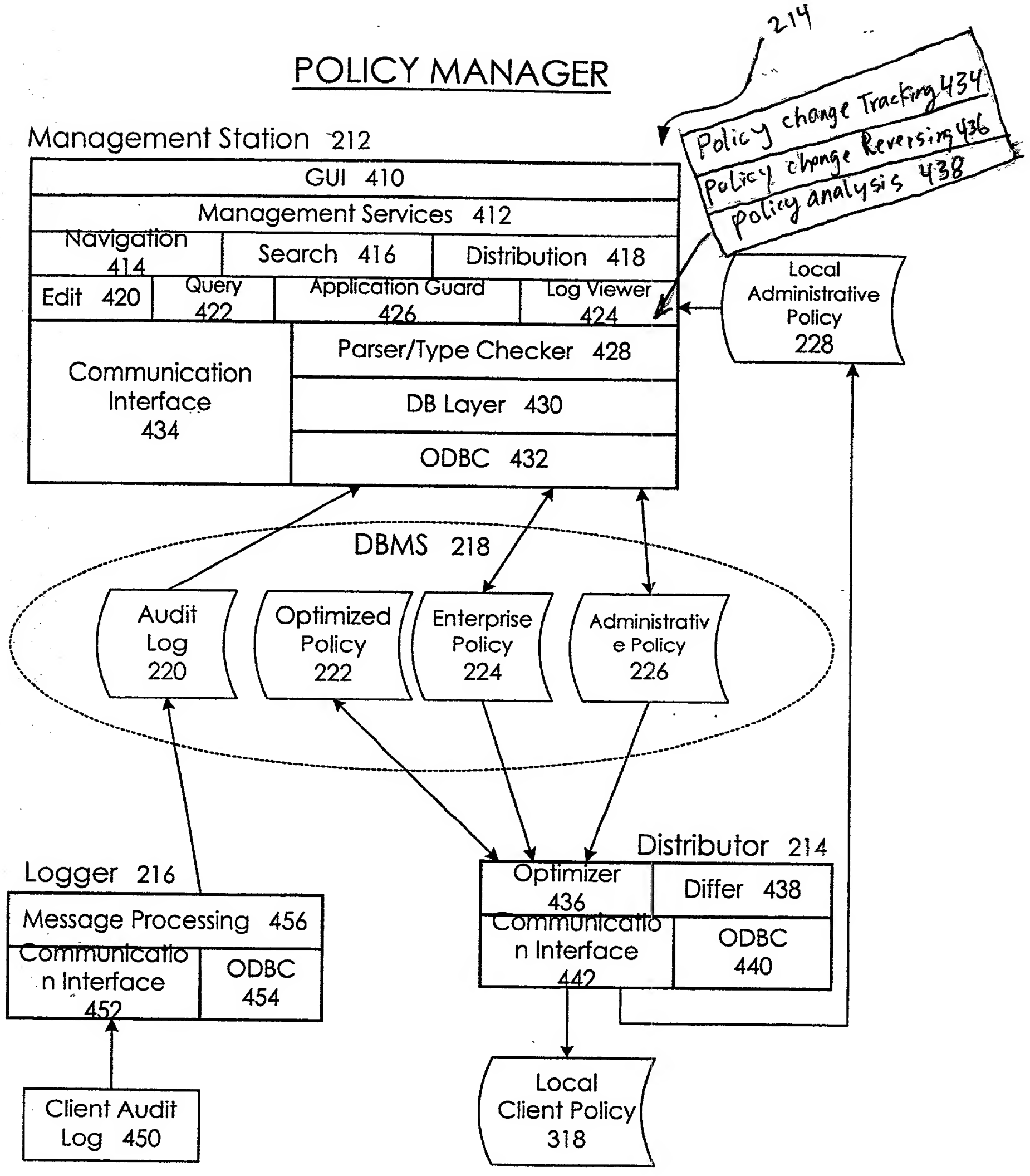

POLICY MANAGER
214
Policy change Tracking 434
Policy change Reversing 436
Policy analysis 438
Management Station 212
GUI 410
Management Services 412
Navigation 414
Search 416
Distribution 418
Edit 420
Query 422
Application Guard 426
Log Viewer 424
Local Administrative Policy 228
Communication Interface 434
Parser/Type Checker 428
DB Layer 430
ODBC 432
DBMS 218
Audit Log 220
Optimized Policy 222
Enterprise Policy 224
Administrative Policy 226
Distributor 214
Optimizer 436
Differ 438
Communication Interface 442
ODBC 440
Logger 216
Message Processing 456
Communication Interface 452
ODBC 454
Client Audit Log 450
Local Client Policy 318

FIG. 4

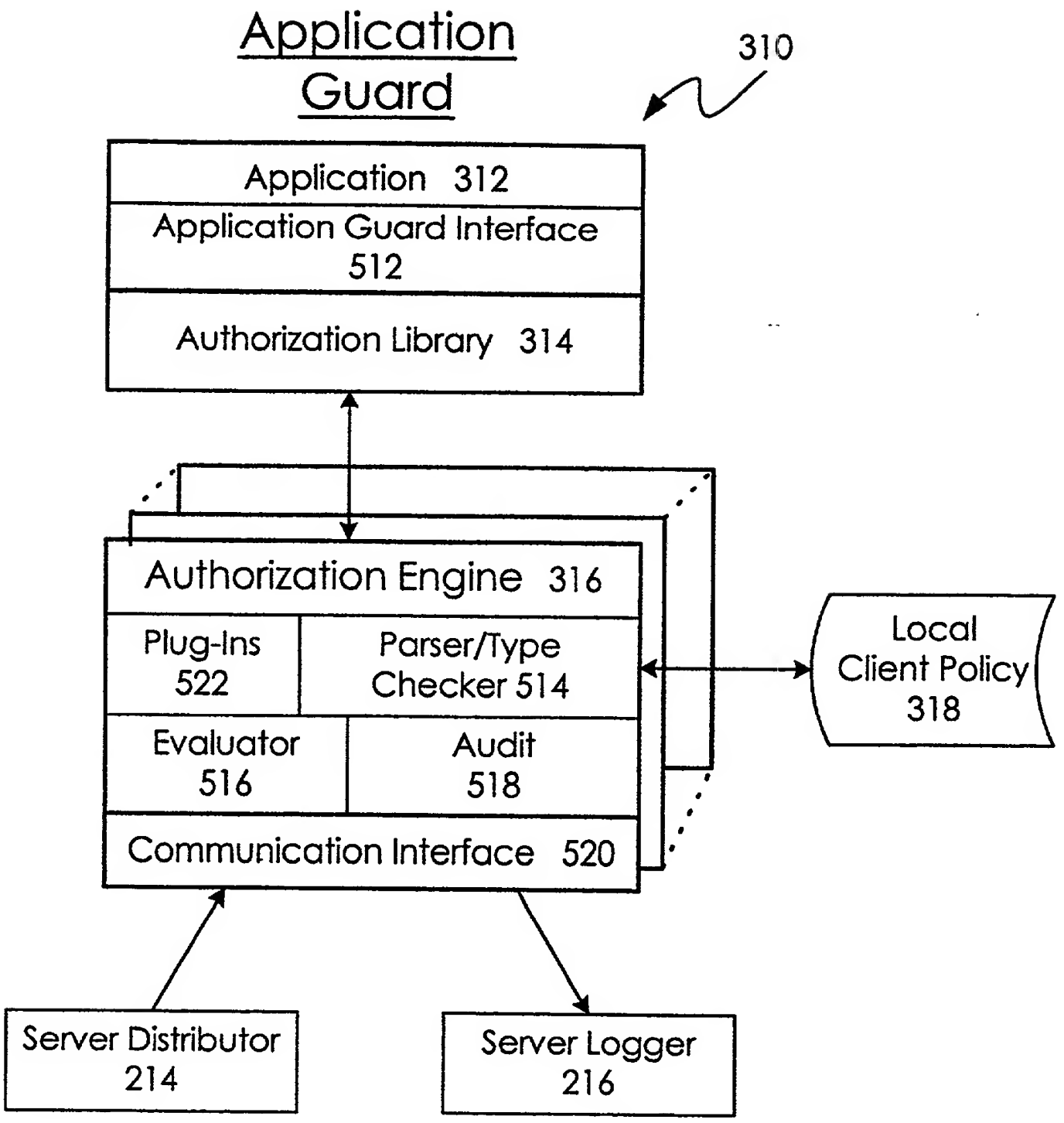

Application Guard
310
Application 312
Application Guard Interface 512
Authorization Library 314
Authorization Engine 316
Plug-Ins 522
Parser/Type Checker 514
Evaluator 516
Audit 518
Communication Interface 520
Local Client Policy 318
Server Distributor 214
Server Logger 216

FIG. 5

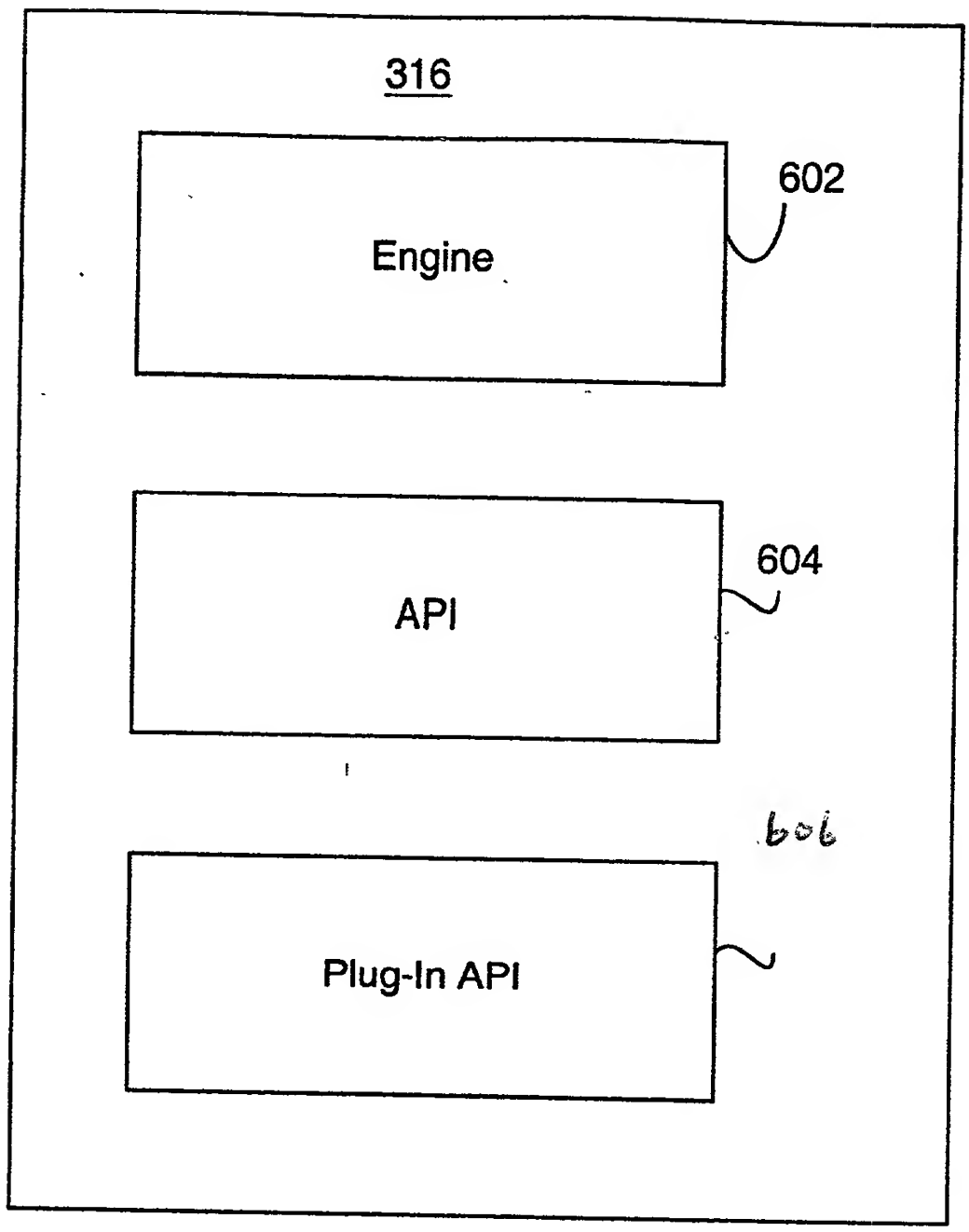


FIG. 6

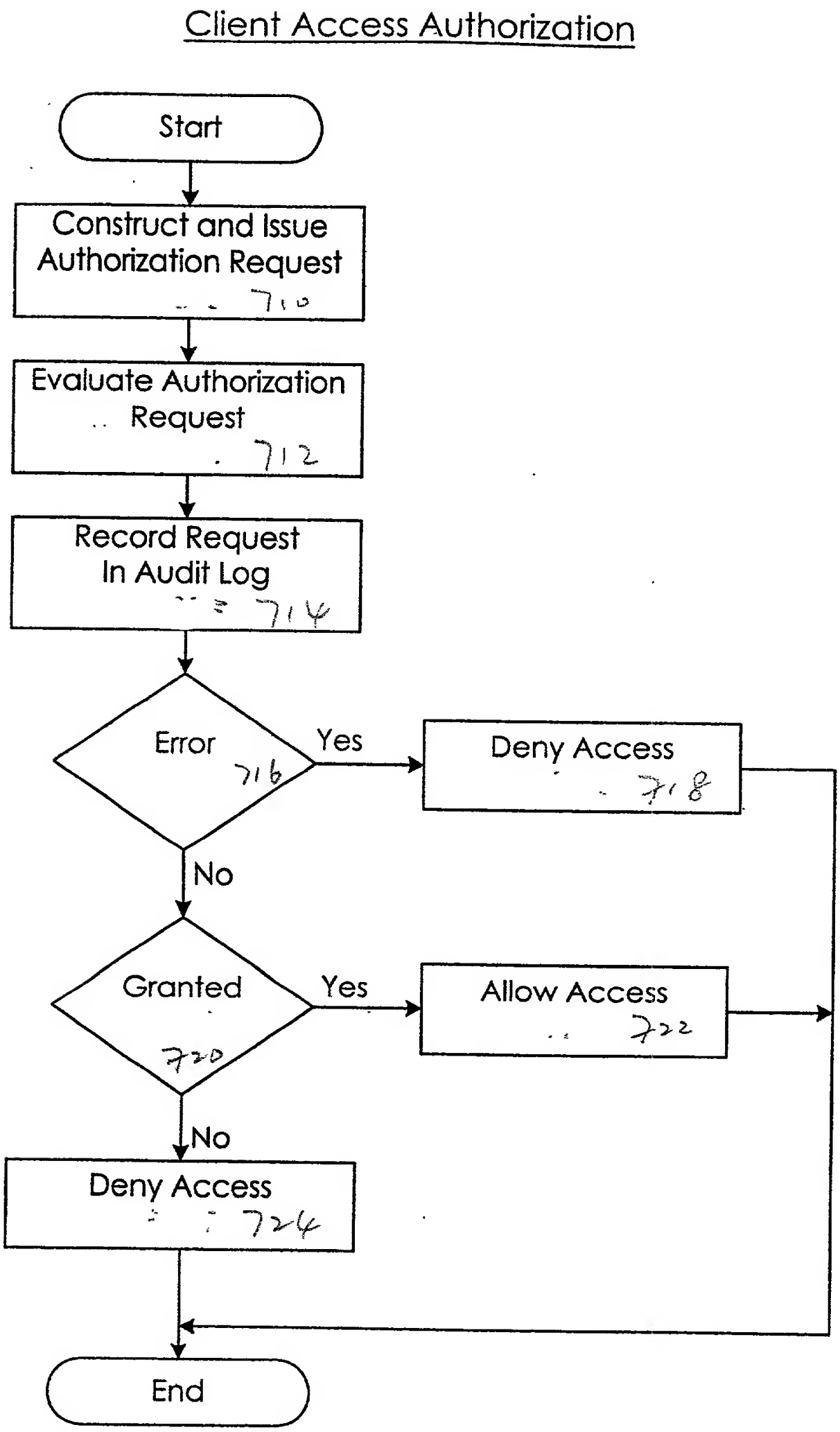

Client Access Authorization
Start
Construct and Issue Authorization Request
710
Evaluate Authorization Request
712
Record Request In Audit Log
714
Error
716
Yes
Deny Access
718
No
Granted
720
Yes
Allow Access
722
No
Deny Access
724
End

FIG. 7

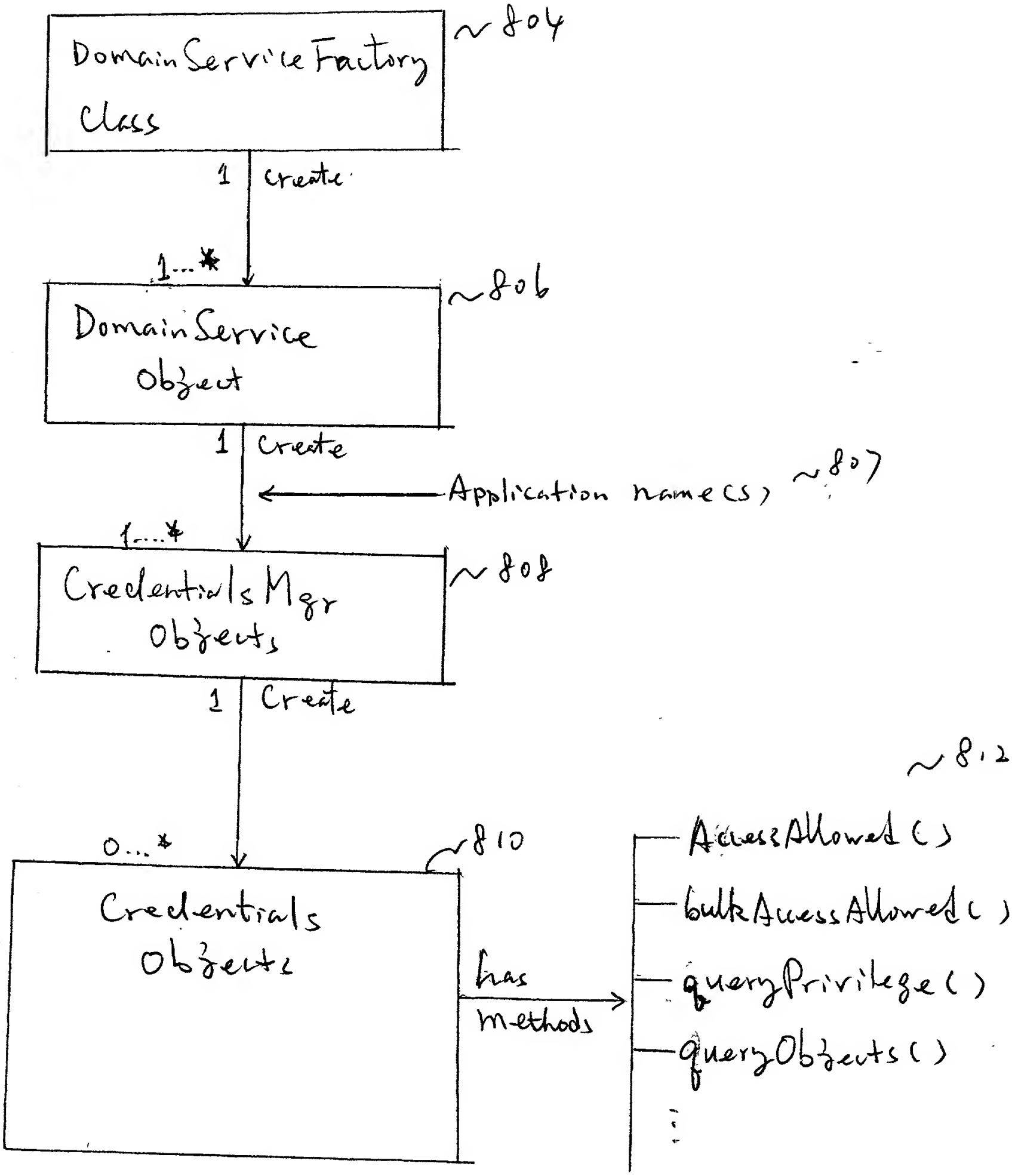

DomainServiceFactory Class
~804
1
create
1...*
DomainService Object
~806
1
Create
Application name(s)
~807
1...*
CredentialsMgr Objects
~808
1
Create
~812
0...*
~810
Credentials Objects
has methods
AccessAllowed()
bulkAccessAllowed()
queryPrivilege()
queryObjects()
...

FIG. 8

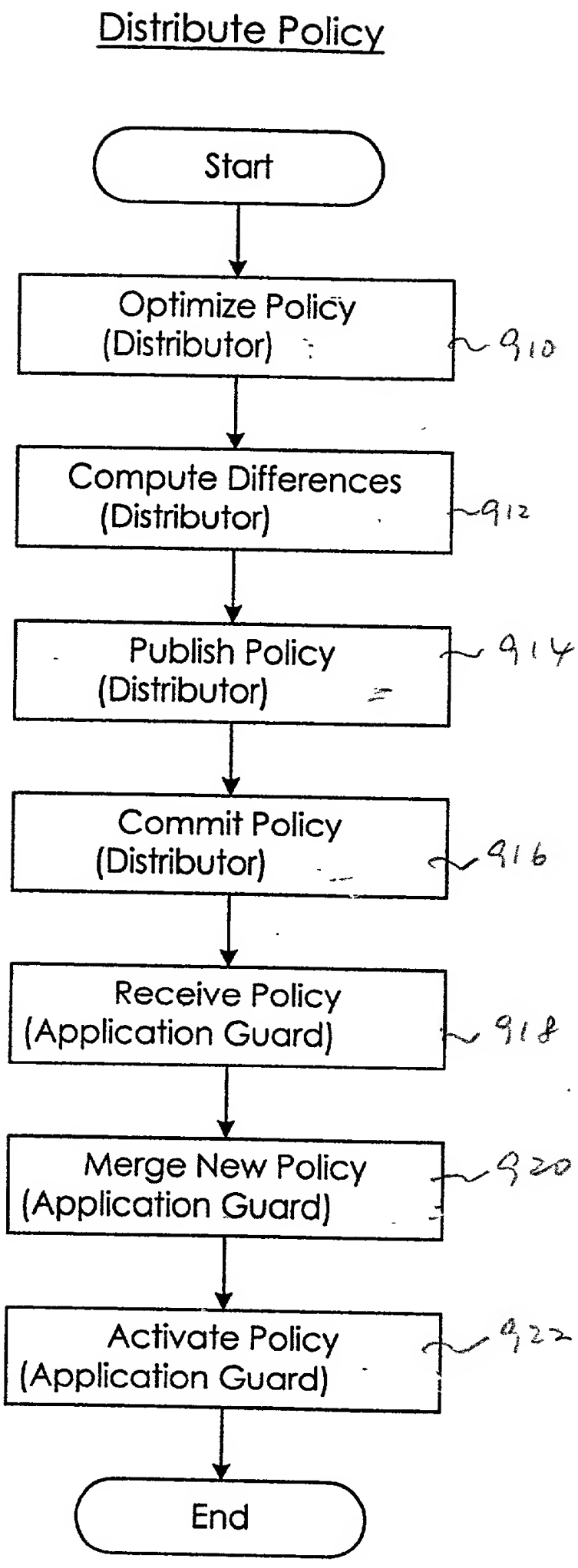
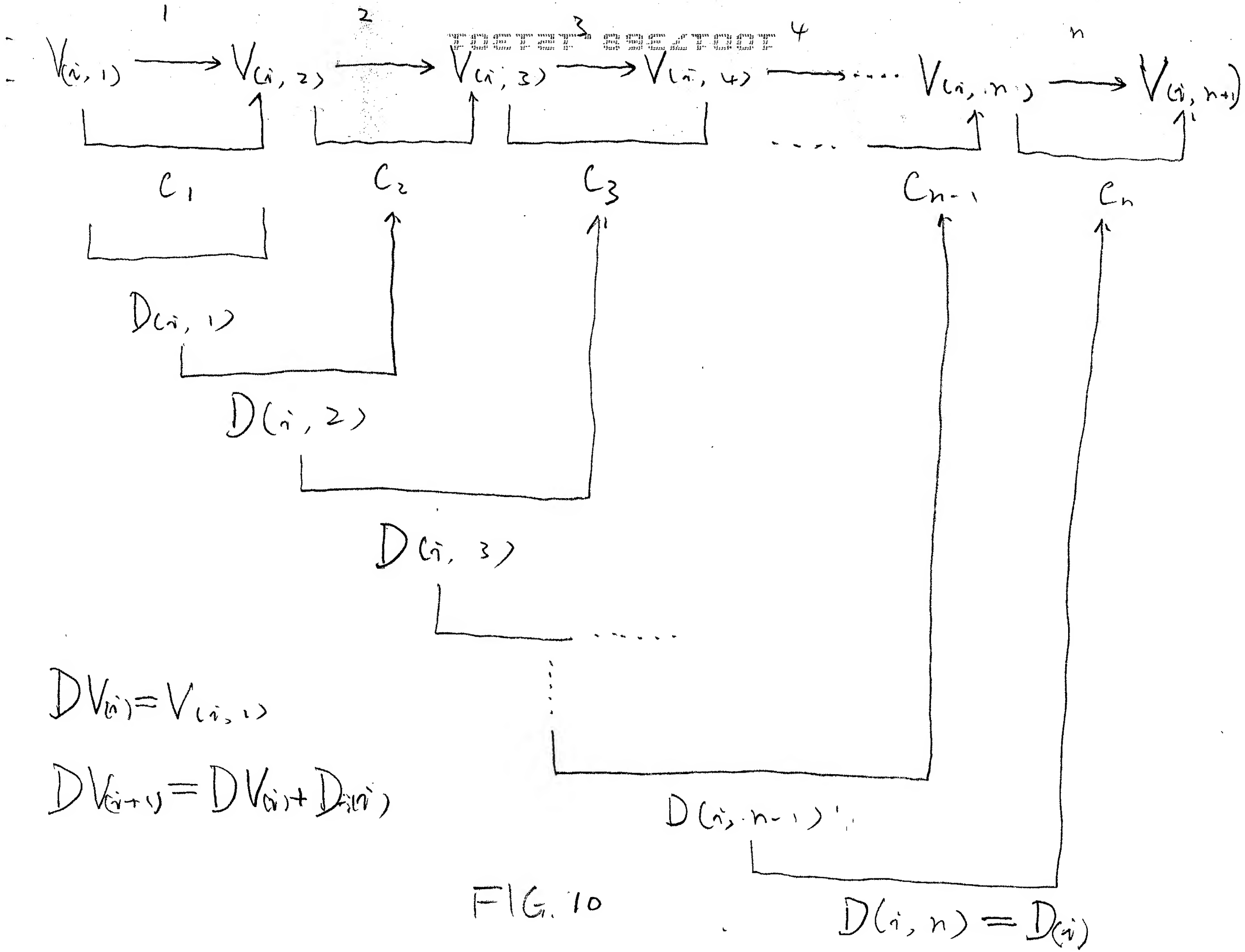

Distribute Policy
Start
Optimize Policy (Distributor)
910
Compute Differences (Distributor)
912
Publish Policy (Distributor)
914
Commit Policy (Distributor)
916
Receive Policy (Application Guard)
918
Merge New Policy (Application Guard)
920
Activate Policy (Application Guard)
922
End

FIG. 9



$DV_{(i)} = V_{(i,1)}$

$DV_{(i+1)} = DV_{(i)} + D_{(i)}$

FIG. 10

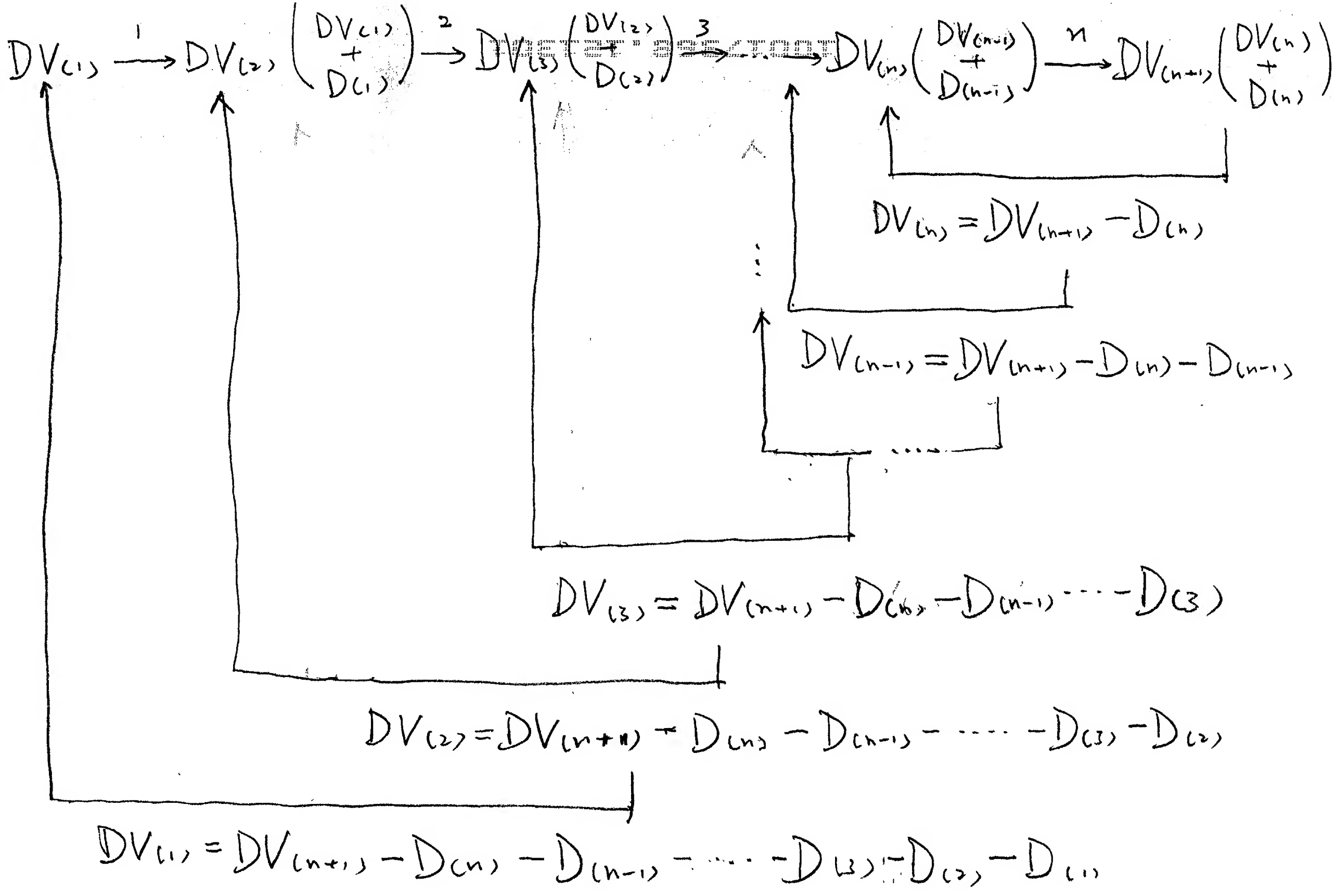

DV(1)
1
DV(2)
DV(1) + D(1)
2
DV(3)
DV(2) + D(2)
3
DV(n)
DV(n-1) + D(n-1)
n
DV(n+1)
DV(n) + D(n)
DV(n) = DV(n+1) − D(n)
DV(n-1) = DV(n+1) − D(n) − D(n-1)
DV(3) = DV(n+1) − D(n) − D(n-1) ··· − D(3)
DV(2) = DV(n+1) − D(n) − D(n-1) − ··· − D(3) − D(2)
DV(1) = DV(n+1) − D(n) − D(n-1) − ··· − D(3) − D(2) − D(1)

FIG. 11

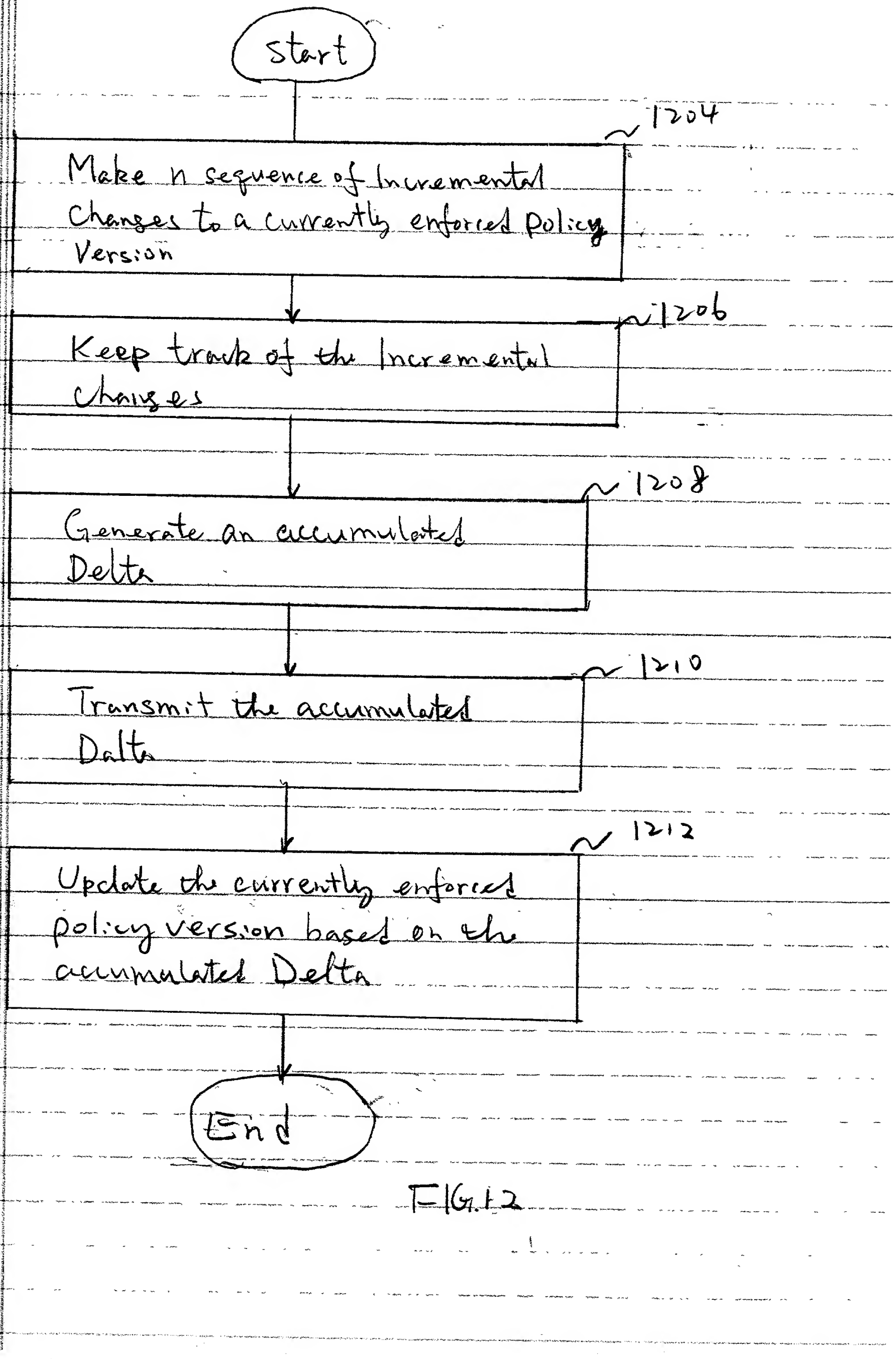

Start
1204
Make n sequence of Incremental Changes to a currently enforced Policy Version
1206
Keep track of the Incremental Changes
1208
Generate an accumulated Delta
1210
Transmit the accumulated Dalta
1212
Update the currently enforced policy version based on the accumulated Delta
End

FIG. 12

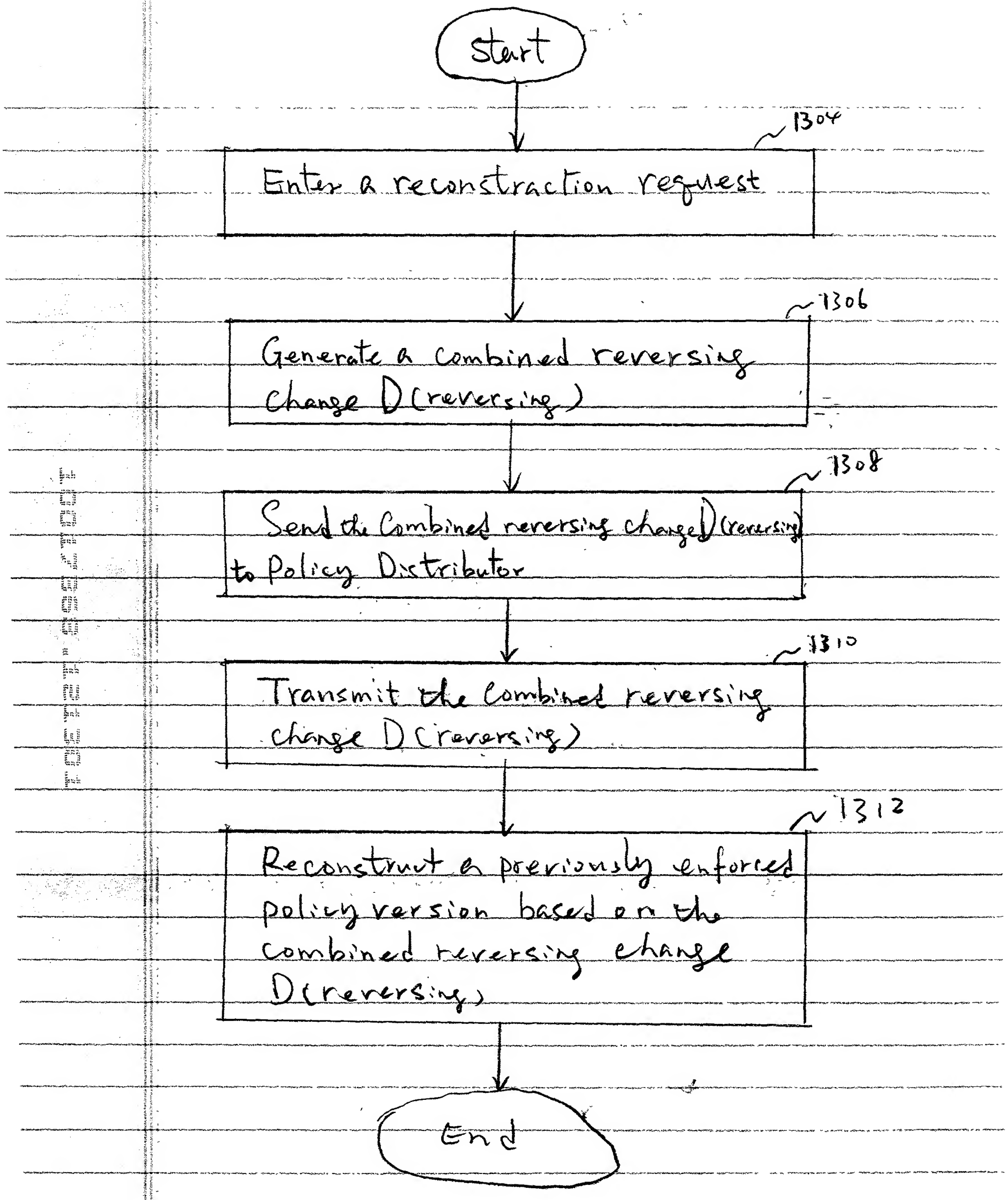

Start
1304
Enter a reconstraction request
1306
Generate a combined reversing change D(reversing)
1308
Send the Combined reversing change D(reversing) to Policy Distributor
1310
Transmit the Combined reversing change D(reversing)
1312
Reconstruct a previously enforced policy version based on the combined reversing change D(reversing)
End

FIG. 13

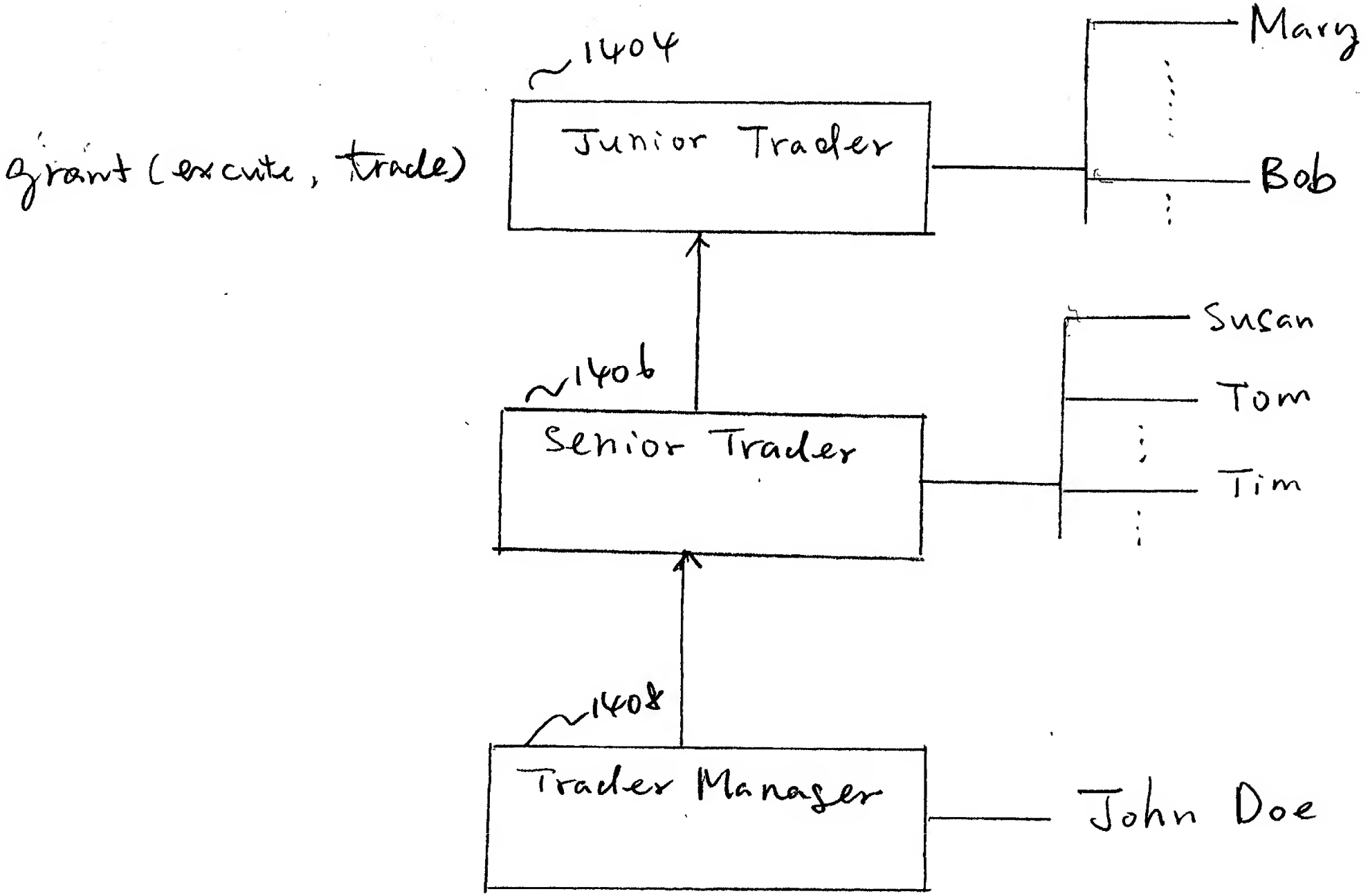

grant (execute, trade)
1404
Junior Trader
Mary
Bob
1406
Senior Trader
Susan
Tom
Tim
1408
Trader Manager
John Doe

FIG. 14

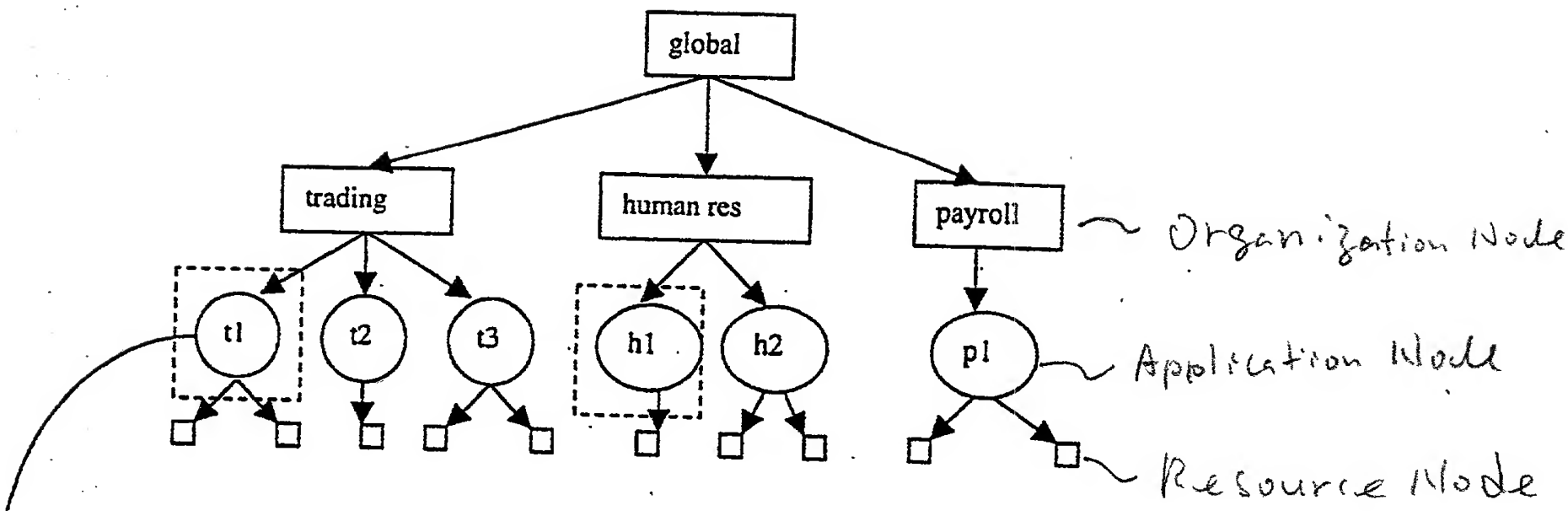

global
trading
human res
payroll
t1
t2
t3
h1
h2
p1
Organization Node
Application Node
Resource Node

FIG. 15

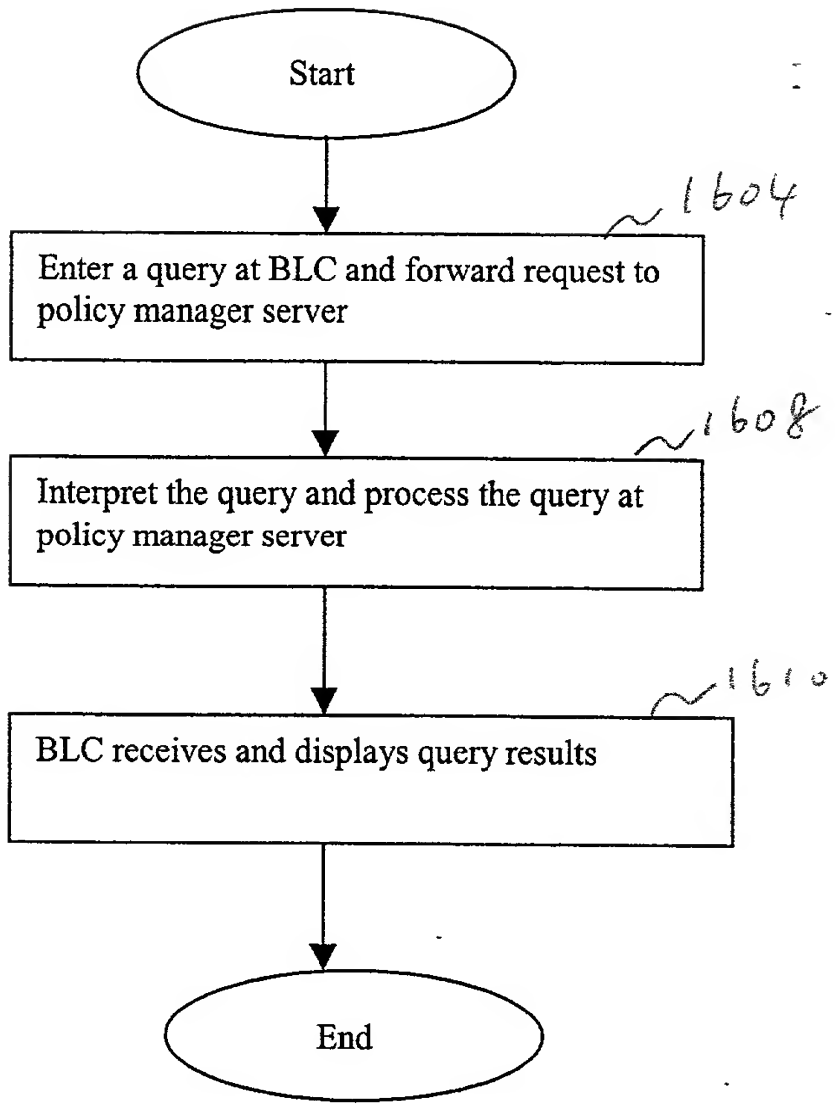

Start
1604
Enter a query at BLC and forward request to policy manager server
1608
Interpret the query and process the query at policy manager server
1610
BLC receives and displays query results
End

FIG. 16

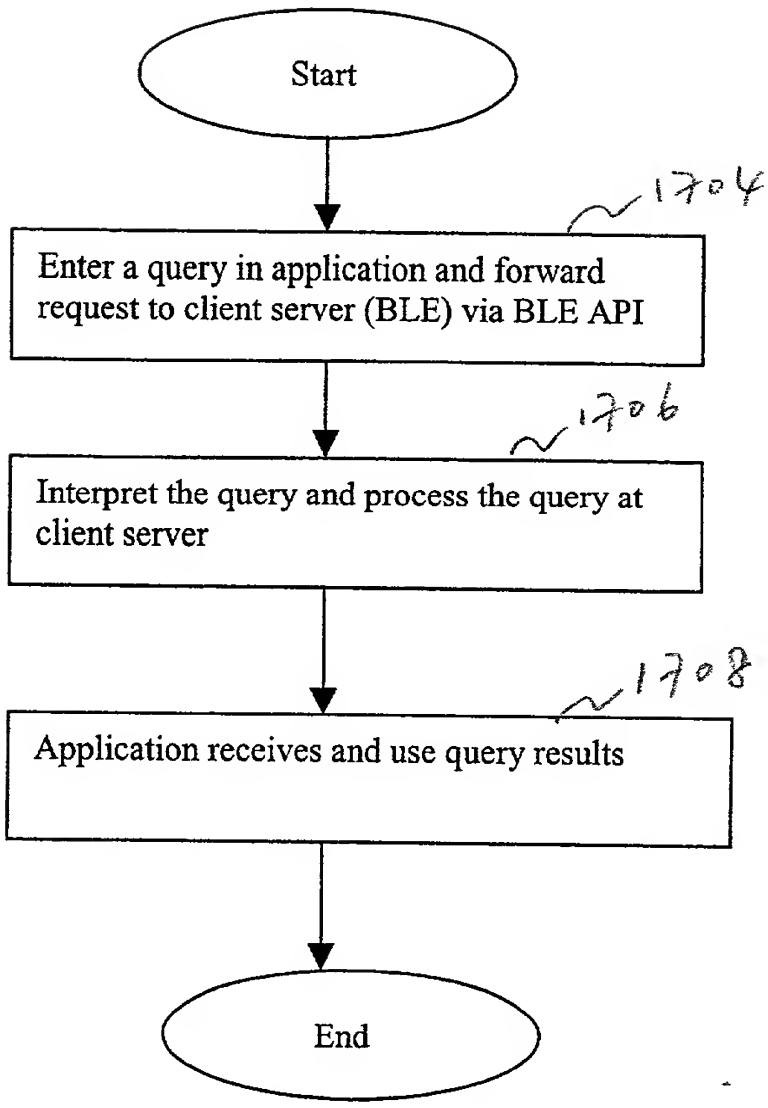

Start
1704
Enter a query in application and forward request to client server (BLE) via BLE API
1706
Interpret the query and process the query at client server
1708
Application receives and use query results
End

FIG. 17